Capstone Engagement

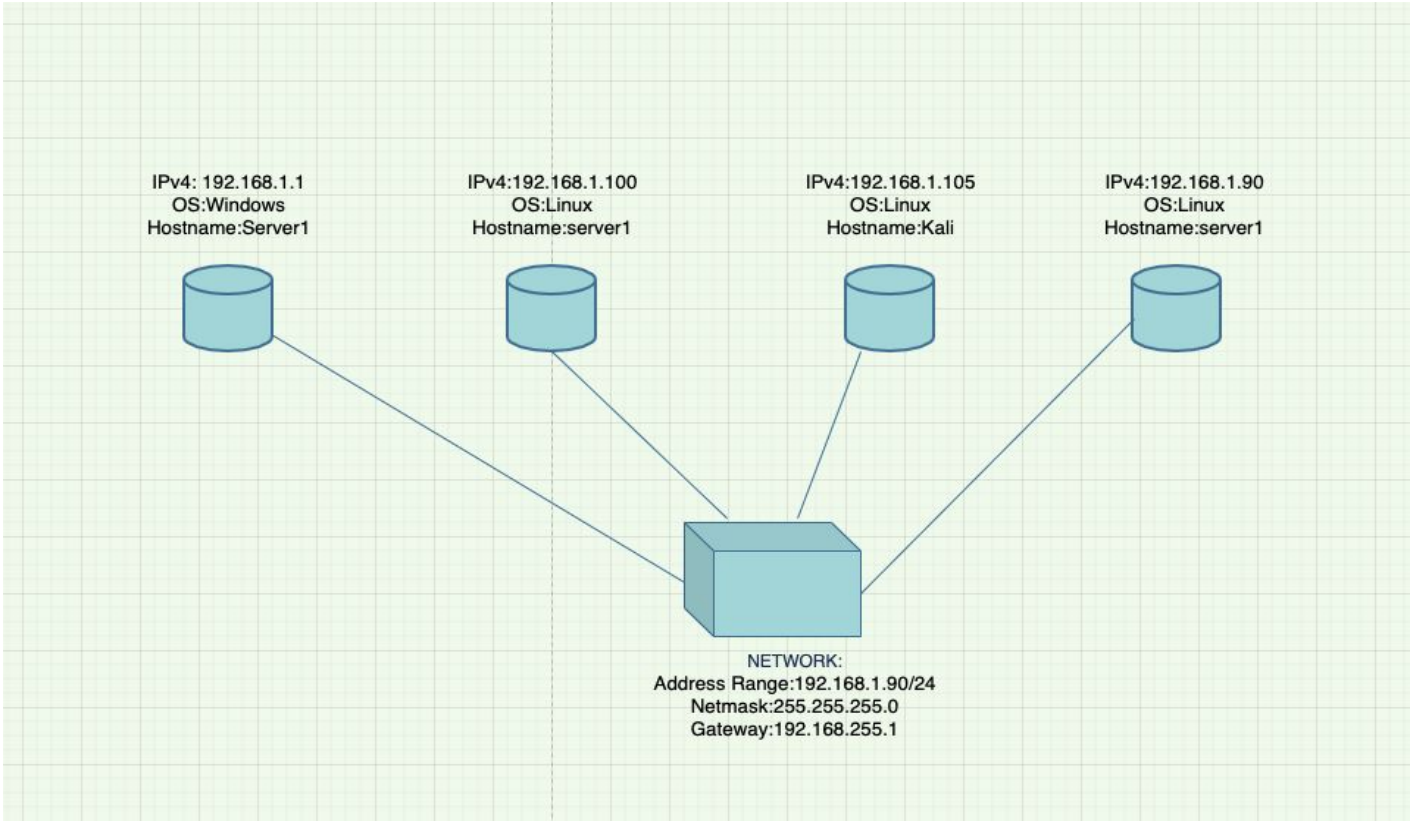
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:192.168.1.90/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.1
OS:Windows
Hostname:Server1

IPv4:192.168.1.100
OS:Linux
Hostname:server1

IPv4:192.168.1.90
OS:Linux
Hostname:server1

IPv4:192.168.1.105
OS:Linux
Hostname:Kali

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Server1	192.168.1.1	Windows server
Server1	192.168.1.100	ELK server
Server1	192.168.1.105	Apache server
Kali	192.168.1.90	Linux server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2019-13386	Allows attackers to execute a shell command and obtain a reverse shell with user privileges.	This vulnerability allows attackers to execute a remote shell on the victim machine
CVE-2007-2767	Hydra Password cracker that allows arbitrary code execution via unknown vectors	This gives the attacker to gain access to the users password files among others
CVE-2020-7384	Msfvenom framework allows malicious user to craft and publish a file that would execute arbitrary commands on the victim machine	This allows the attacker to execute commands and also allows for sensitive file access.
Nmap Port Scanning	Allows port scanning by scanning internet protocols. (TCP, UDP, SCTP, ICMP)	Send packets to verify if ports are open on the target.

Exploitation: Hydra

01

Tools & Processes

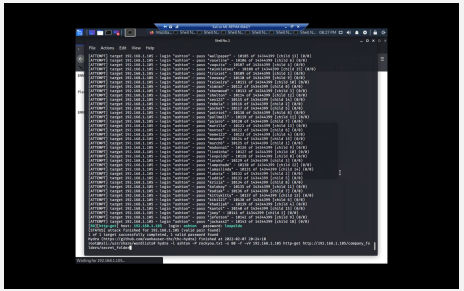
Hydra was used to brute force the password associated with the secret_folder. A hydra script was used using the credentials of the website.

02

Achievements

The exploit by brute force found the password for the account allowing access to the secret_folder.

03



Exploitation: Msfvenom

01

Tools & Processes

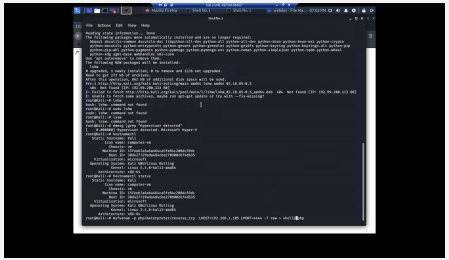
Msfvenom was used to craft a custom script for a reverse shell on the victim machine. This was accomplished through the use of the metasploit framework for execution of the payload.

02

Achievements

The upload of the malicious code into the victims machine.

03



Exploitation: Metasploit

01

Tools & Processes

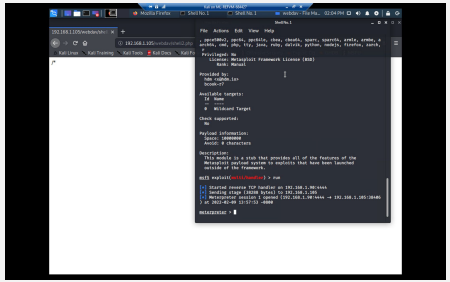
Acts as the handler for the custom script and will run the script with an exploit handler.

02

Achievements

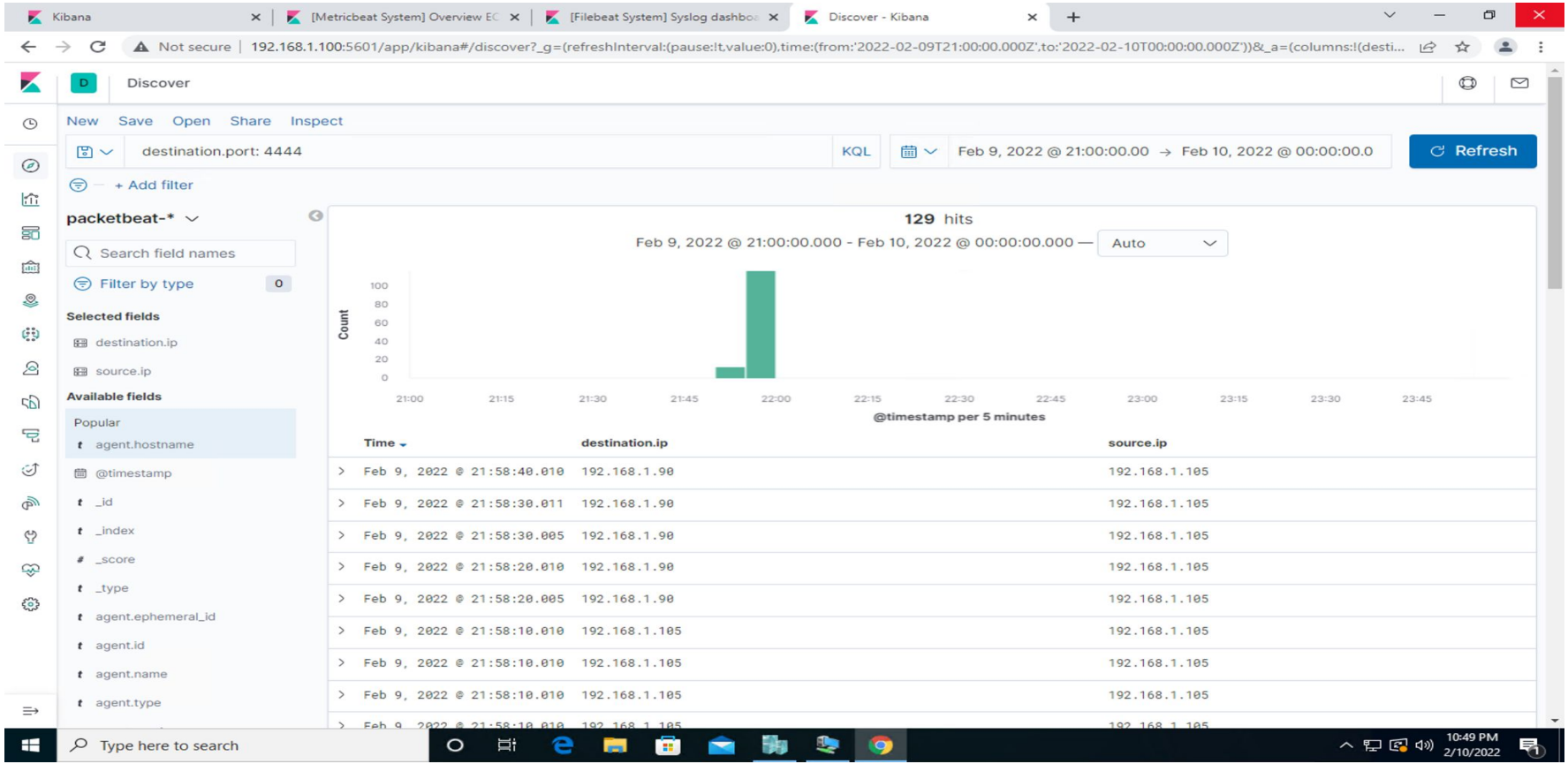
Achieved a meterpreter shell on the victim machine and had access to all file systems.

03

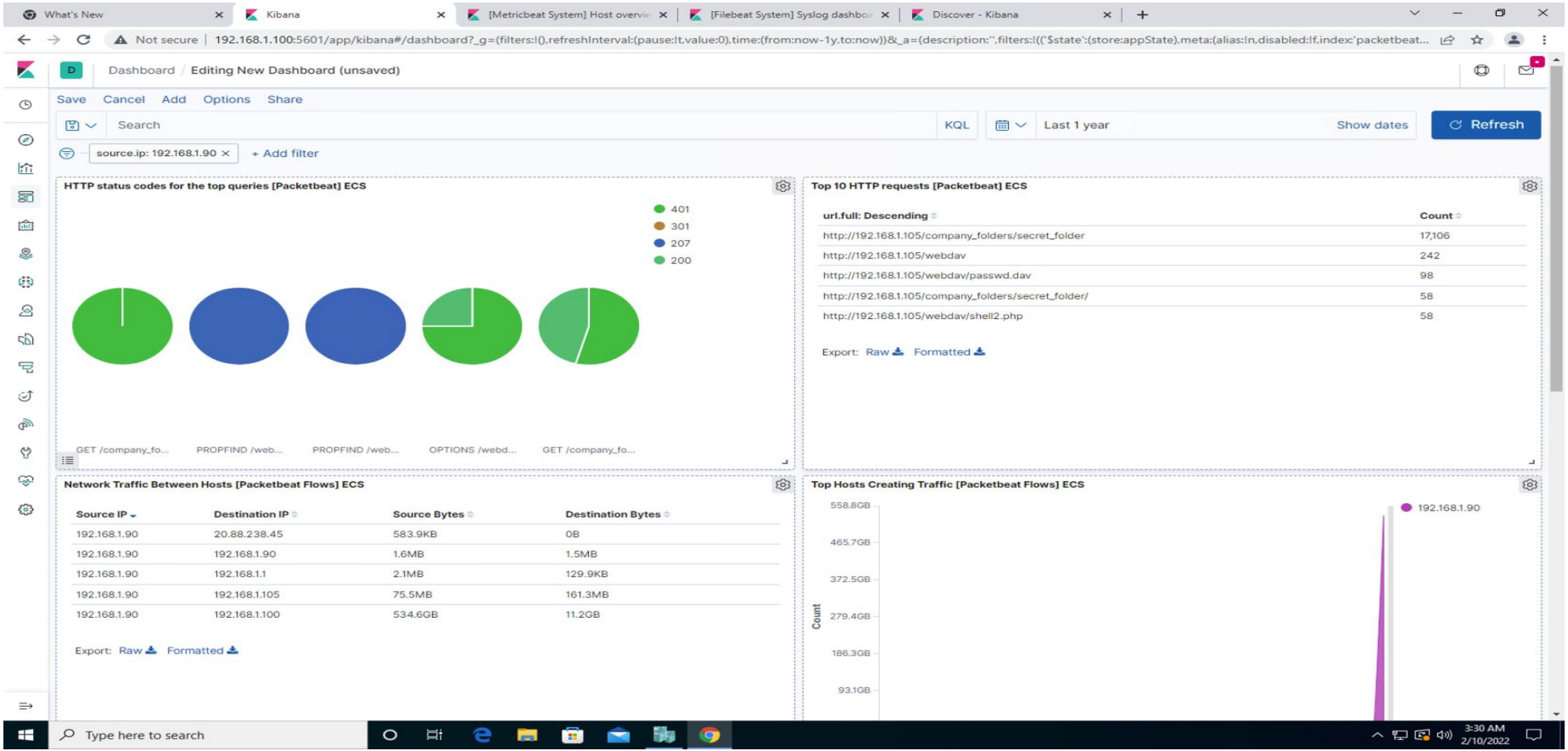


Blue Team
Log Analysis and Attack Characterization

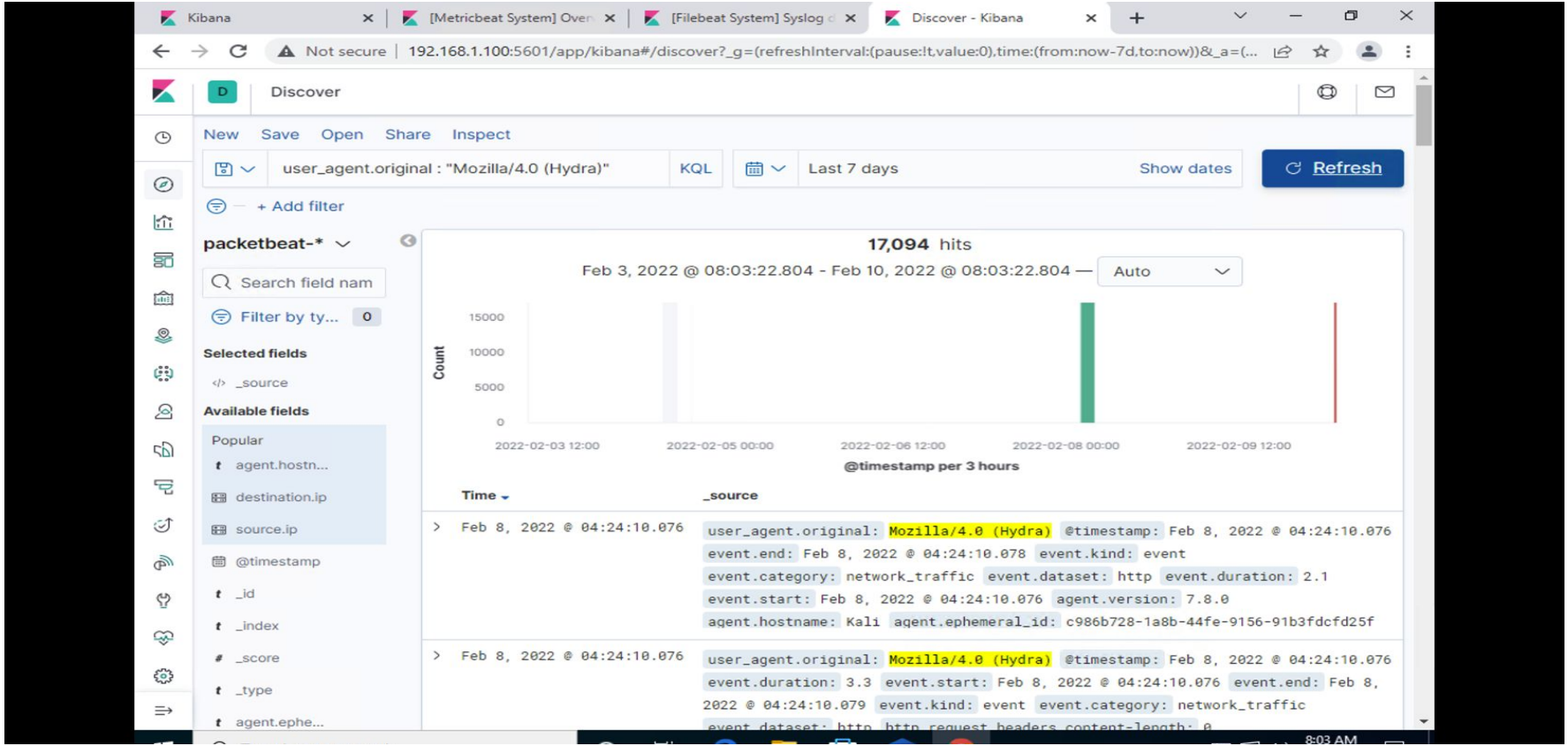
Analysis: Identifying the Port Scan



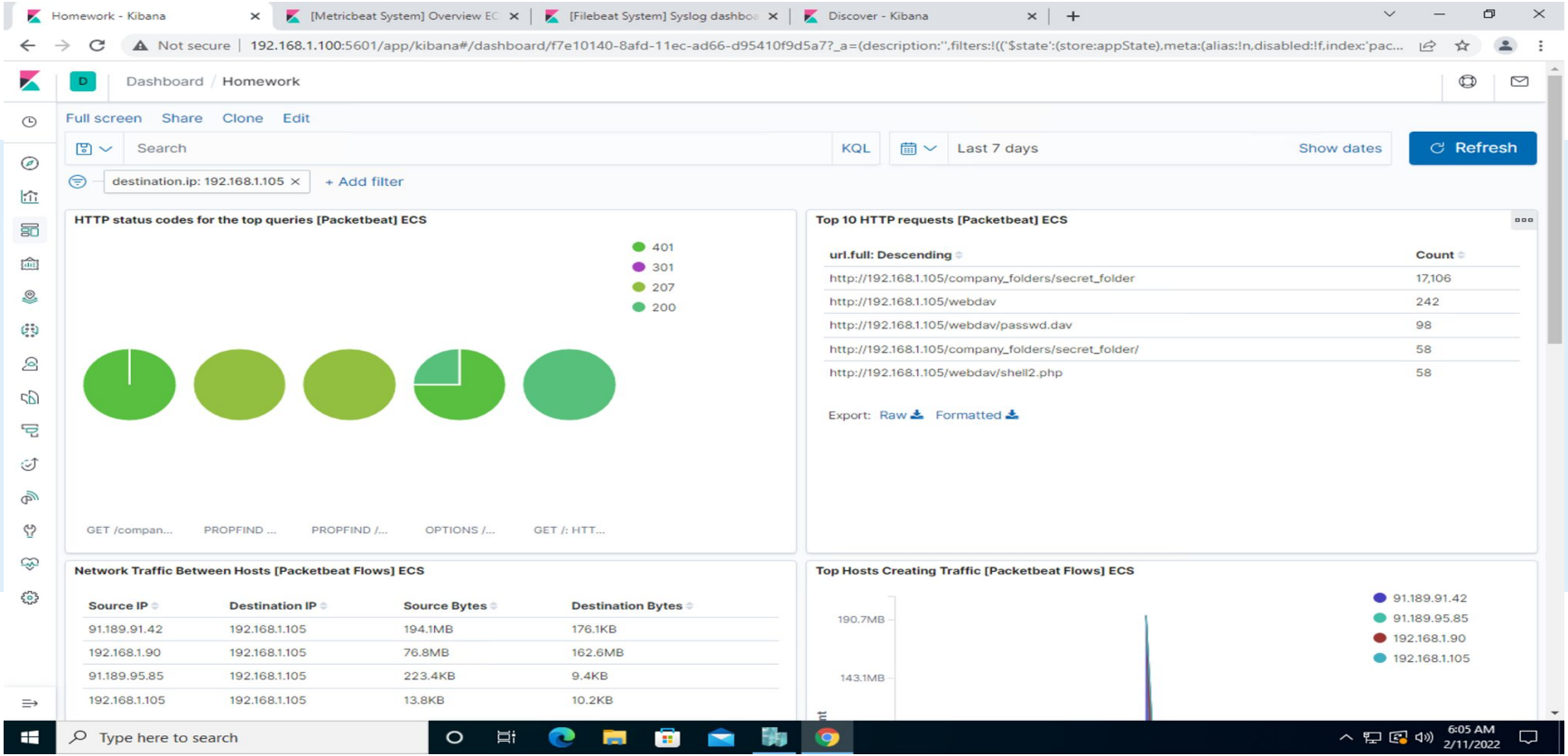
Analysis: Finding the Request for the Hidden Directory



Analysis: Uncovering the Brute Force Attack



Analysis: Finding the WebDAV Connection



Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set an alarm to detect excessive request on any port from an unknown IP on the network.

The alarm would need to be set when the count reaches above 300,000.

System Hardening

A firewall configuration would need to be set to drop incoming unknown syn packets

Mitigation: Finding the Request for the Hidden Directory

Alarm

The alarm would need to be set up for when there are excessive error messages.

The threshold would need to be set at 300,000.

System Hardening

Remove the hidden directory and its corresponding files. This would eliminate the attacker even getting the information.

.

Mitigation: Preventing Brute Force Attacks

Alarm

Set an alarm for excessive http requests.

The threshold would need to be set at 5,000

System Hardening

Configure the system to block all unknown HTTP requests from untrusted sources

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm would need be to created to detect abnormal traffic to the connection.

This alarm threshold would need to be set at >35.

System Hardening

What configuration can be set on the host to control access?

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm can be set to detect an incoming connection to port 4444 and to detect file uploads through this port.

File upload threshold should only be 1

System Hardening

Block all incoming traffic on port 4444 as well as file uploads from this port


The End